Maintaining Security Patches

The Problem We Can No Longer Afford To Ignore!

David Bobart
Acting Chief Security Officer
Information Technology and Communications Division
Department of Public Safety and Correctional Services

Presentation Outline

- The Security Problems
- The Targets
- The Threats
- The Challenge
- Approaches and Philosophies
- Discussion

The Security Problems

- Poorly written software
- Buffer overflow
  1. What is it?
  2. What does it do?

The Targets

- Windows (all flavors)
  - Sheer number of hosts provides ample targets
  - Poorly written software
  - Business practices have created bias in the hacking community
- Linux
  - Large number of installations
  - Choice of those who are opposed to Windows
  - Favorite platform of the hacking community
  - Used to come with too many services activated by default. This is changing…
  - Source code freely and readily available

The Targets

- The UNIXes (Solaris, AIX, Irix, HP-UX)
  - Main targets of hacking for many years as the entire Internet was running on and being maintained by these types of hosts
- Novell
  - Pioneer of directory services
  - Didn't become a real target until IP adopted over IPX
- MacOS
  - Used to be secure because they provided no IP-based network services, but now they are UNIX with UNIX problems

The Threats - Worms

What's the difference between a worm and a virus?

A virus spreads among files on a single system. The mission of a worm is to propagate itself across the network.

The Threats - Worms

Network-based Worms:

- Nimda (several targets to attack)
- Code Red (MS IIS)
- Slammer (MS SQL Server)
- Blaster (MS RPC)
- Welchia (MS RPC)

The Threats - Worms

Email-based Worms (mass mailers):

- SoBig (MS Outlook)
- Mimail (MS Outlook)

Hybrids (the latest):

- Swen/Gibe (MS Internet Explorer)

The Threats – Automated Penetration Scripts

- Automated approach to breaking into computers
- Prior to recent worm successes, this was the most popular and effective method for hackers
- Available to experts and novices (script kiddies)
- Indiscriminate hacking…everyone is a target

The Threats – Focused Penetration Attempts

- Someone has decided that you are the target!
- Dwarfed by sheer number of worm-related infections and automated system compromises
- Very popular among patriotic hackers…very annoying to government agencies

The Challenge

- Over 4000 vulnerabilities reported to CERT in 2002
- Software complexity increasing
- Quality Assurance programs at major software providers are obviously not effective. Additionally, programmers consider quality and security obstacles to the two most important goals which are speed to market and number of features.

The Challenge

- Efficiency of worms is increasing
- Infection isn't an "if" but a "when"
- Estimates:
  - Code Red in 6/2001 doubled its infections every 37 minutes
  - Slammer (SQL Server worm) doubled its infections every 8.5 seconds. It peaked in just 3 minutes at which point it was scanning 55 million hosts per second.

Approaches and Philosophies

Patch Testing

- We can't rely on the vendors!
- Avoid "Patch and Pray" scenario

Approaches To Testing

Ideal Situation:

- Test bed that simulates environment
- Reference systems configured with same hardware and software as production systems
- All versions of production software represented
- After each patch is installed, regression testing is done on systems and applications to ensure that unmodified programs are still operational

Approaches To Testing

Realistic Situation:

- Small group of machines that represent the spectrum of systems in the environment
- Use a single server to test multiple application software packages
- After each patch is installed, do as much regression testing as is possible with limited replica of production environment
- Bulk of security patches impact software that is highly abstracted from the machine hardware so replicating hardware environment isn't as important
- Do your best!

Approaches To Testing

Discussion?

Approaches to Patch Management (PM)

Approaches to Patch Management

Windows Login Script Approach

- Catches all users as they login
- Can target select users or groups
- Cheap from a software perspective
- Requires expertise
- Free products such as KiXtart (www.kixtart.org) extend the capabilities of the login script
- Commercial tools such as ScriptLogic improve upon KiXtart
- Downside – users will be delayed when they first login

Approaches to Patch Management

Windows Logoff Script Approach

- Not popular
- Most people are in a hurry when logging off

Approaches to Patch Management

Automated Patch Management

- Automated patching of devices
- You select who, what, where, and when
- May require the installation of a client on each workstation depending on product
- Most PM packages can check for updates, check for conflicts, and support roll back
- Can generate nice configuration reports!
- Expensive!

Approaches to Patch Management

Many products to choose from:

- LANDesk
- Ecora Patch Manager
- PatchLink Update
- UpdateExpert
- HFNetChkPro

And many more…

Approaches to Patch Management

Caveats

- Automation of patching doesn't mean automatic, nor should it!
- Need to test and distribute patches in a controlled fashion
- Wide Area Network (WAN) and Local Area Network (LAN) bandwidth
- Something that is the responsibility of the vendor is being passed on as an additional software and maintenance cost to the consumer!

Approaches to Patch Management

Discussion?

Patching Philosophies

Patching Philosophies

Patch, Patch, Patch!

(Proactive and aggressive)

Patching Philosophies

- Promoted by the vendors who have released patch management software
- Only possible in environments that have purchased PM software
- Protects you from published vulnerabilities but at what cost?

Patching Philosophies

Patch As Little As Possible

Patching Philosophies

- Security policies will protect you!
- Best practices will protect you!
- Cadbury egg approach to security
- Only a small percentage of vulnerabilities lead to attacks
- Don’t have the time
- Don’t have the resources

Patching Philosophies

Hybrid Approach

(Leverage what you have, install when you must)

Patching Philosophies

- Install patches that are critical and mitigate an immediate threat – you have an IIS server that is accessible to the Internet and a vulnerability is announced – you had better patch it
- After the appropriate testing, install other security patches that pose an ongoing threat
- Implement and enforce security policy
- Establish and implement best practices – it's hard for the Code Red worm to infect your Exchange server when you turned off Microsoft IIS because you didn't need it (if you don't need it, turn it off)

Patching Philosophies

- Make sure every system has active, maintained, and aggressive anti-virus software installed that checks for a new signature file at least every 3 days
- Limit outbound traffic through your Internet firewalls – you may get a mass mailer worm, but if you limit outbound SMTP, you won't allow it to spread
- Implement internal filtering on router interfaces
- Limit change to your environment and therefore promote user sanity

Patching Philosophies

Caveats – Hybrid Approach

- You still need PM software
- You must understand your environment and have the expertise to manage the increased complexity
- You need to be able to craft policies and best practices, and have the management support to implement them

Patching Philosophies

Discussion?

Maintaining Security Patches

Thanks for attending the session!

dbobart@dpscs.state.md.us